IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA

ALABAMA FAMILY FOOT CLINIC, PC; DESERT ABA SOLUTIONS LLC; UNIQUE INTEGRATED CARE; RIVERBEND COUNSELING SERVICES; E5 THERAPY; KIDSTUFF CHILD AND FAMILY COUNSELING PC; UROLOGICAL CONSULTANTS OF FLORIDA; BALL'S REXALL DRUGS, INC., D/B/A B&W REXALL DRUGS; CLOE CHIROPRACTIC CENTER; MIND GARDEN, LLC; SERENITY THERAPY, LLC; PITTSBURG INTERNAL MEDICINE PA; GIEVERS-ZUNIGA FOOT & ANKLE CENTER; KAJAL GEHI PSYCHOTHERAPY, LLC; IRWIN COUNSELING SERVICE, PLLC; LAKE ACUPUNCTURE LLC; DIABETES & ENDOCRINE INSTITUTE; SOUTH CITY COUNSELING STL; NANCY FISH LCSW, MPH; SERENITY COUNSELING CENTER NJ LLC; ROBERT MULLAN, DPM, INC.; WITH GRACE MENTAL HEALTH COUNSELING PLLC; ANEW U COUNSELING SERVICES, PLLC; CULTIVATING MIND LLC; THE WELLIFE, LLC; KAITLIN HECKMAN LLC; REBECCA WILLIAMS, MS, NCC, LPC; HEELEX LLC; BODY MIND & SPINE CHIROPRACTIC; CORE COUNSELING AND CONSULTATION; and FOUR WINDS COUNSELING LLC; individually and on behalf of all others similarly situated,

Plaintiffs,

v.

UNITEDHEALTH GROUP INCORPORATED, CHANGE HEALTHCARE INC., and OPTUM, INC.,

Defendants.

Case No. 24-2335

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs Alabama Family Foot Clinic, PC; Desert ABA Solutions LLC; Unique Integrated Care; Riverbend Counseling Services; E5 Therapy; KidStuff Child and Family Counseling PC; Urological Consultants of Florida; Ball's Rexall Drugs, Inc., D/B/A B&W Rexall Drugs; Cloe Chiropractic Center; Mind Garden, LLC; Serenity Therapy, LLC; Pittsburg Internal Medicine PA; Gievers-Zuniga Foot & Ankle Center; Kajal Gehi Psychotherapy, LLC; Irwin Counseling Service, PLLC; Lake Acupuncture LLC; Diabetes & Endocrine Institute; South City Counseling STL; Nancy Fish LCSW, MPH; Serenity Counseling Center NJ LLC; Robert Mullan, DPM, Inc.; With Grace Mental Health Counseling PLLC; Anew U Counseling Services, PLLC; Cultivating Mind LLC; The Wellife, LLC; Kaitlin Heckman LLC; Rebecca Williams, MS, NCC, LPC; Heelex LLC; Body Mind & Spine Chiropractic; Core Counseling and Consultation; and, Four Winds Counseling LLC ("Plaintiffs"), bring this proposed class action suit, individually and on behalf of all others similarly situated, against Defendants Change Healthcare Inc. ("Change"), Optum, Inc. ("Optum"), and UnitedHealth Group Incorporated ("UHG") (collectively, "Defendants"), and, based on the investigation of counsel, personal knowledge and information and belief, allege as follows:

I. INTRODUCTION

1. This proposed class action suit arises from a cyberattack that has been called "the most significant and consequential incident of its kind against the U.S. healthcare system in history" (the "Data Breach").[1] On February 21, 2024, Defendant Change

[1] *See AHA Statement on HHS Response to Change Healthcare Cyberattack,* (Mar. 5,

experienced a data breach and ransomware attack that crippled the nation's healthcare system and continues to have repercussions today. For several weeks, healthcare providers were not paid for claims they submitted before the ransomware attack and could not submit new claims, although they continued to treat patients. Healthcare providers rely on the payments to run their practices, including paying for medical supplies and employees. The ransomware attack was entirely foreseeable, and Defendants could have easily prevented it by implementing basic cybersecurity measures and having an adequate response and business continuity plan in place. Defendants' UHG, Optum, and Change's conduct deprived healthcare providers across the United States—including Plaintiffs and proposed Class members—of billions of dollars in reimbursements for services rendered and has imposed substantial additional costs and operational burdens on healthcare providers.

2. Defendants control computer networks, including data processing systems, portals, and platforms, that serve as critical infrastructure for administering healthcare services across the United States. Defendants' computer networks process billions of healthcare transactions annually and perform more than one hundred functions used by over one million healthcare providers, including hospitals, physicians, therapists, pharmacies, and laboratories, thereby affecting the delivery of medical care for many millions of Americans. Through aggressive acquisition and expansion, Defendants, headed by corporate parent UHG, have broadened the reach of their services to include: (1) systems that healthcare providers use to submit claims for payment to insurers and other payors, (2)

2024), https://www.aha.org/press-releases/2024-03-05-aha-statement-hhs-response-change-healthcare-cyberattack.

platforms that verify individuals' insurance coverage, (3) programs used to verify prior authorizations for medical treatment and prescription drugs, and (4) dozens of other functions critical to the provision of healthcare services. Change, acquired by UHG and merged with Optum in 2022, is central to the performance of those functions.

3. Hackers gained access to Change's data and computer networks beginning on February 12, 2024 by using compromised login credentials to remotely access a Change Healthcare Citrix "portal" that was not protected by multifactor authentication or MFA—a standard cybersecurity control that should have protected all of Change's internet-facing systems. Once inside Defendants' computer networks, for the next nine days, hackers roamed Change's internal systems, exploring unrestricted folders and files containing sensitive information from providers across the healthcare industry, as well as source code files for Change's healthcare services. During that extended period, the hackers exfiltrated volumes of information which they selected for maximum vulnerability, sensitivity, and value. The hackers also modified and compromised Change's internal systems, including Change's backup systems, to bring them under the hackers' direct control.

4. Members of a well-known cybercriminal organization going by the name of ALPHV/BlackCat ("BlackCat") perpetrated the cyberattack. They were undetected by any security measure implemented by Defendants, even though BlackCat could have been detected, or even stopped at the door, had Defendants implemented basic cybersecurity precautions such as MFA. Given the group's reputation for extracting valuable data, installing ransomware to lock critical systems, and extorting a ransom from its victims, the FBI, the Department of Health and Human Service's Office of Information Security and

Healthsector Cybersecurity Coordination Center, and other authorities specifically and repeatedly urged the healthcare industry to implement specific precautions, as early as April 2022, to prevent and protect against data breach and ransomware attacks by this specific organization. Defendants did not heed these warnings.

5. After nine days of exploring and extracting some of the nation's most sensitive, valuable healthcare data, on or around February 21, 2024, BlackCat announced its presence by triggering the ransomware it had installed during its extended foray. The ransomware, consistent with the group's normal methods, locked Defendants out of Change's internal systems. The lockout extended to Change's backup systems, which were surprisingly not kept in a secure location, another standard practice designed to protect from this type of cyberattack. BlackCat then threatened to sell the exfiltrated data on the dark web and to continually block access to Change's systems unless UHG acceded to their demands and paid a ransom. Ultimately, UHG paid a $22 million ransom.

6. Defendants also lacked reasonable incident response measures and a business continuity plan for this scenario. Realizing the security vulnerabilities in Change's systems, Defendants took the most extreme measure they could; they disabled and disconnected Change's systems nationwide. Defendants' actions halted insurance authorizations for medical treatments, claims processing, and payments for approximately one-third of healthcare transactions in the United States. For over a month, there was a total cessation of critical services. During the total shutdown, pre-existing claims that healthcare providers had submitted for payment went unpaid; to the extent new claims could be made, they went unprocessed; and, numerous standard functions required to provide healthcare services,

such as insurance pre-authorizations, could not be obtained. Defendants began to restore certain services in late March 2024, but the process has been slow, and problems continue to persist. UHG's CEO testified before Congress that the backup systems that Defendants were locked out of were the root cause of the delay in getting the Change services up and running.

7. The impact of Defendants' actions on hard-working medical providers who provide critical care to patients around the country was disastrous. The unavailability of Change's mission-critical services resulted in unpaid claims, overdue payments, interest accumulation, inability to perform eligibility verifications leading to loss of services, increased administrative costs caused by manual processes, negative credit impact, and other harms. Within weeks of the onset of the outage, the American Hospital Association ("AHA") described the situation as a "staggering loss of revenue."[2] According to some estimates, by mid-March, providers were losing between $500 million and $1 billion in revenue *daily* because of the shutdown. By late March, healthcare providers faced a backlog of over $14 billion just in unpaid and unprocessed claims, severely impairing their ability to make payroll, order supplies, and otherwise fund their operations. Rick Pollack, President and CEO of the AHA, remarked that the Data Breach is the "most serious incident of its kind leveled against a U.S. healthcare organization." Many medical providers around

[2] *See* Richard J. Pollack, *AHA Urges More Congressional Action to Help Providers Affected By Change Healthcare Cyberattack*, AMERICAN HOSPITAL ASSOCIATION (Mar. 13, 2024), https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack.

the country have been pushed to the edge of bankruptcy and have been forced to delay or deny vital medical treatments needed by patients around the county.

8. Defendants compounded problems for providers, and the healthcare industry in general, by withholding important information and refusing to provide an accurate timeline for restoring Change's services, among many other shortcomings and failures. Upon learning that Change's backup systems had been compromised, Defendants knew and must have known that providers should turn to Defendants' competitors to maintain at least some of their normal operations. But Defendants withheld that fact, instead suggesting to struggling providers, day after day, that services may be restored the next day. Even today, Defendants still have not provided a conclusive date by which they intend to bring all provider accounts and services current.

9. The cyberattack, and the need for an incident response and business continuity plan in the event of a successful attack, were foreseeable. The healthcare industry has been a target of cyberattacks for years given the massive amount of confidential personal health information ("PHI") and personal identifying information ("PII") that healthcare organizations collect, store, and maintain and that can be used to commit identity theft. Since as early as 2014, government agencies have warned the healthcare industry about the threat of cyberattacks and have repeatedly cautioned them to ensure that their systems are secure and protected. The U.S. government had also specifically warned the industry that BlackCat had hit at least seventy organizations since December 2023, a majority of which were healthcare organizations.

10. Defendants could have easily prevented the attack and the catastrophic events that followed with basic industry-standard cybersecurity, threat detection and incident response measures, by following an appropriate business continuity plan, and by specifically implementing measures recommended to thwart BlackCat's standard tactics, techniques, and procedures, which were well known from attacks in prior years. Given their position as providers of critical infrastructure in the nationwide delivery of healthcare, Defendants knew they were high-profile targets that needed to implement incredibly robust cybersecurity controls. Instead, Defendants neglected to implement even basic industry-standard technical and administrative cybersecurity controls, such as MFA. Indeed, Defendant UHG's policy is to use MFA for all externally facing systems, however, it did not enforce that policy in all of its organizations as evidenced by the cyberattack and Data Breach.

11. As a result of Defendants' negligence, failures, and omissions, BlackCat—which has been known for some time to target healthcare organizations—was able to easily infiltrate the Change computers networks and steal confidential health data and source code, among other things, revealing the vulnerabilities in Defendants' computer networks that resulted in Change's complete shutdown. The catastrophic impact of Defendants' poor security measures and lack of an incident response, including a business continuity plan, fell upon healthcare providers, including Plaintiffs, who continue to feel the effects today.

12. Plaintiffs, individually and on behalf of all others similarly situated, bring this action against Defendants seeking redress for their unlawful and tortious conduct and asserting common law claims for negligence, negligence *per se*, negligent interference with

prospective economic advantage, breach of contract, unjust enrichment, and for violations of the state consumer protection statutes identified herein. Through these claims, Plaintiffs seek damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems and incident response planning.

II. PARTIES

13. Plaintiff Alabama Family Foot Clinic, PC is a citizen of Alabama and maintains its principal place of business in Rainbow City, Alabama.

14. Plaintiff Desert ABA Solutions LLC is a citizen of Arizona and maintains its principal place of business in Yuma, Arizona.

15. Plaintiff Unique Integrated Care is a citizen of Arizona and maintains its principal place of business in Tempe, Arizona.

16. Plaintiff Riverbend Counseling Services is a citizen of California and maintains its principal place of business in Sacramento, California.

17. Plaintiff E5 Therapy is a citizen of California and maintains its principal place of business in Suisun City, California.

18. Plaintiff KidStuff Child and Family Counseling PC is a citizen of Colorado and maintains its principal place of business in Loveland, Colorado.

19. Plaintiff Urological Consultants of Florida is a citizen of Florida and maintains its principal place of business in North Miami, Florida.

20. Plaintiff Ball's Rexall Drugs, Inc., D/B/A B&W Rexall Drugs is a citizen of Florida and maintains its principal place of business in Inverness, Florida.

21. Plaintiff Cloe Chiropractic Center is a citizen of Illinois and maintains its principal place of business in Mt. Vernon, Illinois.

22. Plaintiff Mind Garden, LLC is a citizen of Indiana and maintains its principal place of business in Indianapolis, Indiana.

23. Plaintiff Serenity Therapy, LLC is a citizen of Iowa and maintains its principal place of business in Dubuque, Iowa.

24. Plaintiff Pittsburg Internal Medicine PA is a citizen of Kansas and maintains its principal place of business in Pittsburg, Kansas.

25. Plaintiff Gievers-Zuniga Foot & Ankle Center is a citizen of Maryland and maintains its principal place of business in Olney, Maryland.

26. Plaintiff Kajal Gehi Psychotherapy, LLC is a citizen of Massachusetts and maintains its principal place of business in Woburn, Massachusetts.

27. Plaintiff Irwin Counseling Service, PLLC is a citizen of Michigan and maintains its principal place of business in Jackson, Michigan.

28. Plaintiff Lake Acupuncture LLC is a citizen of Minnesota and maintains its principal place of business in Twin Cities, Minnesota.

29. Plaintiff Diabetes & Endocrine Institute is a citizen of Mississippi and maintains its principal place of business in Flowood, Mississippi.

30. Plaintiff South City Counseling STL is a citizen of Missouri and maintains its principal place of business in St. Louis, Missouri.

31. Plaintiff Nancy Fish LCSW, MPH is a citizen of New Jersey and maintains her principal place of business in Hackensack, New Jersey.

32. Plaintiff Serenity Counseling Center NJ LLC is a citizen of New Jersey and maintains its principal place of business in Freehold Township, New Jersey.

33. Plaintiff Robert Mullan, DPM, Inc. is a citizen of New Mexico and maintains his principal place of business in Las Cruces, New Mexico.

34. Plaintiff With Grace Mental Health Counseling PLLC is a citizen of New York and maintains its principal place of business in Saratoga, New York.

35. Plaintiff Anew U Counseling Services, PLLC is a citizen of North Carolina and maintains its principal place of business in Raleigh, North Carolina.

36. Plaintiff Cultivating Mind LLC is a citizen of Ohio and maintains its principal place of business in Cincinnati, Ohio.

37. Plaintiff The Wellife, LLC is a citizen of Ohio and maintains its principal place of business in North Canton, Ohio.

38. Plaintiff Kaitlin Heckman LLC is a citizen of Pennsylvania and maintains its principal place of business in Pittsburgh, Pennsylvania.

39. Plaintiff Rebecca Williams, MS, NCC, LPC is a citizen of Pennsylvania and maintains its principal place of business in Pittsburgh, Pennsylvania.

40. Plaintiff Heelex LLC is a citizen of Tennessee and maintains its principal place of business in Knoxville, Tennessee.

41. Plaintiff Body Mind & Spine Chiropractic is a citizen of Texas and maintains its principal place of business in Temple, Texas.

42. Plaintiff Core Counseling and Consultation is a citizen of Washington and maintains its principal place of business in Pasco, Washington.

43. Plaintiff Four Winds Counseling LLC is a citizen of Wisconsin and maintains its principal place of business in Middleton, Wisconsin.

44. Defendant Change Healthcare Inc. is a publicly traded company incorporated in Delaware with its principal place of business in Nashville, Tennessee. It became a subsidiary of UnitedHealth Group Incorporated in 2022 and is operated by Optum, Inc., another UHG subsidiary.

45. Defendant Optum, Inc. maintains its principal place of business in Eden Prairie, Minnesota and is incorporated in Delaware.

46. Defendant UnitedHealth Group Incorporated is a Delaware corporation with its principal place of business in Minnetonka, Minnesota. UHG exercises control over the management of the Change cybersecurity systems as evidenced by UHG's response to the Data Breach as alleged herein.

III. JURISDICTION AND VENUE

47. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least one hundred members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which one or more members of the proposed Class, including Plaintiffs, are citizens of a state different from Defendants. The Court has supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the same case or controversy.

48. This Court may exercise jurisdiction over Defendants because they are registered to conduct business in Minnesota; have sufficient minimum contacts in

Minnesota; and, intentionally avail themselves of the markets within Minnesota through the promotion, sale, and marketing of their services, thus rendering the exercise of jurisdiction by this Court proper and necessary.

49. Venue is proper in this District under 28 U.S.C. § 1391 because Defendants Optum, Inc. and UnitedHealth Group Incorporated reside in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District. In addition, the Judicial Panel on Multidistrict Litigation on June 7, 2024, issued an order centralizing litigation arising out of the Change Healthcare data breach in this District.

IV. FACTUAL ALLEGATIONS

A. Factual Background

50. UHG is a healthcare mega-conglomerate that generated $372 billion in revenue in 2023 alone. It operates two primary businesses; the first is UnitedHealthcare, the nation's largest insurer and one of the top three pharmacy benefit managers in the country. The second of UHG's primary business enterprises is Optum, a technology company that provides "health services," leveraging technology and data to provide clinical, administrative, and financial processes for insurers, providers, and others throughout the healthcare industry.

51. Change is a healthcare services company established in 2005 (known as Emdeon before rebranding in 2015), which works across the U.S. health system "to make clinical, administrative and financial processes simpler and more efficient for payers, providers, and consumers." Among other services, Change operates "the nation's largest electronic data interchange (EDI) clearinghouse, which transmits data between healthcare

providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions . . . ."[3]

52. Previously, Change was an independent company that was not owned by any healthcare provider or insurer. In 2021, UHG proposed a deal to acquire Change for a merger with Optum.

53. The merger raised antitrust and data privacy concerns. Melinda Reid Hatton, AHA Vice President and General Counsel, voiced concerns about the proposed deal and wrote to the Department of Justice ("DOJ") asking it to investigate. In the letter to the DOJ, Ms. Hatton wrote, "The proposed acquisition would produce a massive consolidation of competitively sensitive healthcare data and shift such data from Change Healthcare, a neutral third party, to Optum."[4]

54. The DOJ investigated and filed a complaint to stop the acquisition, citing Change's "access to a vast trove of competitively sensitive claims data that flows through its EDI clearinghouse—over a decade's worth of historic data as well as billions of new claims each year."[5]

---

[3] *See* Complaint, *United States et al. v. UnitedHealth Group, Inc. et al.*, No. 22-cv-00481 (D.D.C. Feb. 24, 2022), ECF No. 1.

[4] *See* Donna M. Pocius, *AHA Expresses Opposition to Merger between UnitedHealth Group's OptumInsight and Change Healthcare, DOJ Agrees to Look into the $13B Deal*, DARK DAILY (Apr. 7, 2021), https://www.darkdaily.com/2021/04/07/aha-expresses-opposition-to-merger-between-unitedhealth-groups-optuminsight-and-change-healthcare-doj-agrees-to-look-into-the-13b-deal/.

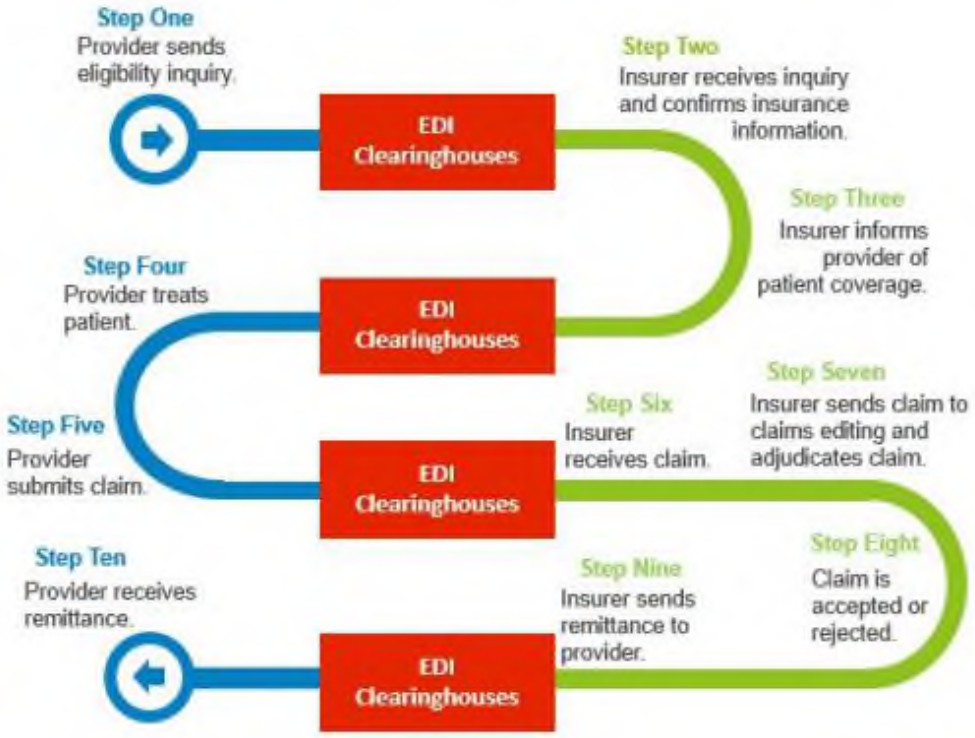
[5] *See* Complaint, *United States et al. v. UnitedHealth Group, Inc. et al.*, No. 22-cv-00481 (D.D.C. Feb. 24, 2022), ECF No. 1.

55. The DOJ, however, lost its challenge to UHG's acquisition of Change after a district judge ruled in UHG's favor and the DOJ chose not to appeal.

56. UHG completed its acquisition of Change in October 2022 and merged it with Optum, announcing in a press release that, "[t]he combined businesses share a vision for achieving a simpler, more intelligent, and adaptive health system for patients, payers, and care providers. The combination will connect and simplify the core clinical, administrative and payment processes health care providers and payers depend on to serve patients. Increasing efficiency and reducing friction will benefit the entire health system, resulting in lower costs and a better experience for all stakeholders."

57. Change's penetration and integration within the United States healthcare system—even prior to consolidation with Optum—is extensive. An estimated 50 percent of all medical claims in the United States pass through Change's EDI clearinghouse alone. As the illustration below shows,[6] EDI clearinghouses such as Change perform at least four crucial functions in the provision of patient care:

[6] *Id.*



58. Change's "pervasive network connectivity," as it described its business in its 2019 S-1 filing when the company went public, impacts "the vast majority of U.S. payers and providers" because Change operates fundamental technological infrastructure connecting "approximately, 2,200 government and commercial payers" with 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories, and processes clinical records for over 112 million unique patients in the United States.[7] According to the company's website, Change processes 15 billion healthcare transactions each year, and its "clinical connectivity solutions" touch a third of U.S. patients.[8]

[7] *See* Form S-1 Registration Statement, Change Healthcare, Inc., https://www.sec.gov/Archives/edgar/data/1756497/000119312519076886/d638353ds1.htm (March 15, 2019).
[8] *See* https://www.changehealthcare.com/ (last visited June 19, 2024).

B. The February 2024 Data Breach and Ransomware Attack

59. Change, a 40-year-old company, had several older legacy technologies that it did not upgrade before the Data Breach. It also failed to implement MFA. On May 1, 2024, UHG's Chief Executive Office testified before Congress that when UHG acquired Change and merged it with Optum, UHG was working to upgrade Change's technologies; UHG, however, failed to implement MFA although it is a basic, standard security measure. It is no surprise then that BlackCat was able to gain access to Change's systems on February 12, 2024.

60. According to the testimony of UHG's CEO before Congress, the hackers used compromised credentials to log into Change's outward-facing remote login application for employees (Change's "Citrix portal"). Since Change's Citrix portal did not require users to complete MFA, such as a one-time code sent to a personal device, or any other identity verification to log in, BlackCat was able to walk right into Change's computer networks.

61. For at least a week after the hackers first accessed Change's systems and databases, Defendants also failed to detect the hackers' exploits. As UHG admits, "Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data."[9] BlackCat's hackers also installed software necessary to perpetrate a ransomware attack.

[9] Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group, Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack," https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf (May 1, 2024).

62. On or around February 21, 2024, Defendants finally became aware that Change's systems and data had been compromised when the hackers deployed ransomware to encrypt critical systems throughout Change's information technology environments, preventing UHG, Optum, and Change from accessing them.

63. Initially, UHG claimed that a nation-state actor was responsible for the Data Breach. On February 28, 2024, however, BlackCat publicly took responsibility. The group has been in operation since November 2021 and its tactics are well-known among cybersecurity professionals. As global cybersecurity company Trend Micro noted in October 2022, "BlackCat ransomware has frequently made the headlines for its successive attacks on high-profile targets."[10] Indeed, BlackCat has been the subject of numerous advisories and warnings from government authorities. The FBI Cyber Division, for example, publicly issues "alerts" and "advisories" to help companies guard against ransomware. In April 2022, the FBI issued a detailed technical advisory about ALPHV/BlackCat, warning businesses that: (1) "BlackCat/ALPHV ransomware leverages previously compromised user credentials to gain initial access to the victim system;" (2) "Once the malware establishes access, it compromises Active Directory user and administrator accounts;" and (3) "BlackCat/ALPHV steals victim data prior to the execution of the ransomware, including from cloud providers where company or client data

[10] *See Ransomware Spotlight BlackCat*, Trend Micro Research, Oct. 27, 2022, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

was stored."[11] The FBI provided technical specifications concerning the characteristics of the group's prior attacks, to facilitate identification of future attacks, and recommended measures to prevent future data breaches and ransomware attacks by ALPHV/BlackCat, urging businesses to:

- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement network segmentation.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.[12]

[11] *See BlackCat/ALPHV Ransomware Indicators of Compromise*, FBI Flash No. CU-000167-MW, https://www.ic3.gov/Media/News/2022/220420.pdf (Apr. 19, 2022).
[12] *Id.*

64. In the April 2022 advisory, the FBI also discouraged businesses that experienced a ransomware attack from paying a ransom, explaining that "[p]ayment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities."[13] The Data Breach here was consistent with the group's widely reported past operations and could have been prevented by implementing even some of the recommended measures above. Indeed, experts have opined that multifactor authentication would likely have prevented the breach.[14]

65. On February 28, 2024, BlackCat announced in a post on its dark web leak site that UHG had lied to the public about the nature and extent of the data breach, and threatened that UHG was "walking on a very thin line."[15] BlackCat described the process it had employed over many days choosing data to exfiltrate as "highly selective," ultimately capturing sensitive Medicare, Tricare, CVS-Caremark, Health Net, MetLife, and numerous private insurance companies' data, which in turn contained millions of individual medical and dental records, insurance records, payment information, telephone numbers, home and email addresses, military personnel records, and Social Security numbers, as well as over 3,000 source code files for Change Healthcare solutions.[16] Below is the statement that

[13] *Id.*
[14] *See, e.g.*, https://www.healthcaredive.com/news/change-healthcare-cyberattack-congress-unitedhealth-andrew-witty/714954/ (June 11, 2024).
[15] Brett Callow (@BrettCallow), X (Feb. 28, 2024, 9:30 AM), https://x.com/BrettCallow/status/1762893128326111404.
[16] *Id.*

BlackCat issued regarding the cyberattack, indicating that the group has reviewed a substantial amount of confidential medical and personal identifying information:

> Change Healthcare - Optum - UnitedHealth
>
> 2/28/2024, 4:19:59 PM
>
> UnitedHealth has announced that the attack is "strictly related" to Change Healthcare only and it was initially attributed to a nation state actor.
>
> Two lies in one sentence.
>
> Only after threatning [sic] them to announce it was us, they started telling a different story.
>
> It is true that the attack is centered at Change Healthcare production and corporate networks, but why is the damage extremely high? Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions. Meaning thousands of healthcare providers, insurance providers, pharmacies, etc . . .
>
> Also, being inside a production network one can imagine the amount of critical and sensitive data that can be found.
>
> We were able to exfiltrate to be exact more than 6 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.
>
> The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:
>
> - Medicare
> - Tricare
> - CVS-CareMark
> - Loomis
> - Davis Vision
> - Health Net
> - MetLife
> - Teachers Health Trust

- Tens of insurance companies and others

Anyone with some decent critical thinking will understand what damage can be done with such intimate data on the affected clients of UnitedHealth/UnitedHealth solutions as well, beyond simple scamming/spamming.

After 8 days and Change Health have [sic] still not restored its operations and chose to play a very risky game hence our announcement today.

So for everyone, both those affected and fellow associates. [sic] to understand what is at stake our exfiltrated data includes millions of:

- active US military/navy personnel PII
- medical records
- dental records
- payments information
- Claims information
- Patients PII including Phone numbers/addresses/SSN/emails/etc ...
- 3000+ source code files for Change Health solutions (for source-code review gents out there)
- Insurance records
- many many more

UnitedHealth you are walking on a very thin line be careful you just might fall over.

PS: For all those cyber intelligence so called expert . . . we did not use ConnectWise exploit as our initial access so you should base your reports you tell people on actual facts not kiddi [sic] speculations.[17]

66. Screenshots, allegedly of the compromised files, were shared on the dark web as proof of the Data Breach.[18] On February 28, 2024, UHG confirmed that the Data Breach

[17] *Id.*

[18] Ashley Capoot, *UnitedHealth paid ransom to bad actors, says patient data was compromised in Change Healthcare cyberattack*, CNBC (Apr. 22, 2024, 6:23 PM),

was perpetrated by BlackCat and later admitted that it paid a ransom to BlackCat, which many reports indicate was for 350 Bitcoin, or approximately $22 million.[19]

67. The stolen data, apparently, is still on the dark web, because on April 7, 2024, Change received a ransom notice from a different group claiming to have the same data, threatening to sell it if Change did not pay a second ransom.[20] UHG admits that the exfiltrated data "could cover a substantial proportion of people in America."[21]

C. The Change Shutdown Has Devastating Effects on Healthcare Providers

68. Soon after Defendants learned of the ransomware attack on or around February 21, 2024, they realized that Change's computer networks were vulnerable and not in compliance with industry standards and legal requirements for the protection of PHI. Defendants immediately and completely "severed connectivity with Change's data centers."[22] A total shutdown continued for a month, with some systems still offline today. During the shutdown and to a significant extent thereafter, previously submitted claims were not paid. Providers could not submit any new claims. Insurance eligibility for new

---

https://www.cnbc.com/2024/04/22/unitedhealth-paid-ransom-to-bad-actors-says-patient-data-was-compromised-in-change-healthcare-cyberattack.html.

[19] *See e.g.*, Gaby Del Valle, *UnitedHealth CEO admits it paid $22 million ransom to BlackCat*, THE VERGE (May 1, 2024, 2:53 PM), https://www.theverge.com/2024/5/1/24146693/unitedhealth-22-million-ransom-ransomware-hack-blackcat (May 1, 2024).

[20] *See Change Healthcare Targeted by Second Ransomware Attack*, PYMNTS (Apr. 14, 2024), https://www.pymnts.com/cybersecurity/2024/change-healthcare-targeted-by-second-ransomware-attack/.

[21] Testimony of Andrew Witty before House Energy and Commerce Committee Subcommittee on Oversight and Investigations, *Examining the Change Healthcare Cyberattack*, https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf (May 1, 2024).

[22] *Id.*

and existing patients could not be verified. The result was chaos for healthcare services around the country. The consequences for both patients and providers have been devastating, leaving many providers on the brink of bankruptcy. Indeed, UHG's CEO recognized in May 2024—almost three months after the ransomware attack—that medical providers are still struggling.

69. Defendants withheld information about the anticipated duration of the outage, which quickly became a matter of great importance to health care providers who relied on Change's services for normal business operations. Beginning in the early morning hours of February 21, 2024, UHG made a series of announcements concerning the incident on the website https://solution-status.optum.com/ suggesting that only a temporary, perhaps day-long, interruption of certain services would occur. UHG's first announcement, posted at 2:15 a.m. ET simply stated that "some applications are currently unavailable." Ten hours later on February 21, 2024, at 12:09 p.m. ET, UHG disclosed that it was experiencing "a network interruption due to a cyber security issue," which, UHG stated, was "expected to last at least through the day." On February 24, 2024, the American Hospital Association issued a security advisory notifying members and the public that "Change Healthcare has not provided a specific timeframe for which recovery of the impacted applications is expected[.]"[23] UHG continued posting vague and generic updates that "a cyber security issue" was expected to cause a disruption "at least through the day"

[23] *See AHA Cybersecurity Advisory*, AMERICAN HOSPITAL ASSOCIATION (Feb. 24, 2024), https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers (emphasis in original).

for a full week, with the last such update posted February 28, 2024 at 5:58 p.m. ET., the same day that BlackCat publicized the nature and severity of the attack, and presumably after the hackers had informed Defendants of their intent to share information with the public.[24]

70. In a letter to Health and Human Services, the AHA stated that while the full scope was "unclear," the AHA expected impacts to be far-reaching given Change's national presence.[25] The AHA also explained how the incident has affected healthcare providers in terms of being unable to collect revenue. "[W]ithout this critical revenue source, hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services," the AHA stated.[26] "In addition, replacing previously electronic processes with manual processes will add considerable administrative costs on providers, as well as divert team members from other tasks. It is particularly concerning that while Change Healthcare's systems remain disconnected, it and its parent entities benefit financially, including by accruing interest on potentially billions of dollars that belong to health care providers."[27] The AHA also recognized that hospitals and health systems "may be experiencing challenges with

[24] *See* Optum Solution Status, https://solution-status.optum.com/incidents/hqpjz25fn3n7 (last visited May 3, 2024).
[25] *See AHA Letter to HHS on Implications of Change Healthcare Cyberattack*, AMERICAN HOSPITAL ASSOCIATION (Feb. 26, 2024), https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack.
[26] *Id.*
[27] *Id.*

obtaining care authorizations for their patients, as well as delays in payment."[28] Antitrust experts have opined that the Data Breach showed why placing "one conglomerate at the center of multiple health care functions is inherently risky."[29]

71. According to the president of Florida Hospital Association, Mary Mayhew, her members built "sophisticated systems that are reliant on Change Healthcare,"[30] and that changing processes could take about 90 days during which they would have no cash flow. "It's not like flipping a switch," said Mayhew.[31]

72. On March 13, 2024, the AHA wrote to Senators Ron Wyden and Mike Crapo about the Data Breach. According to the AHA's letter, the downed systems "are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process."[32]

---

[28] *Id.*

[29] *See* Brittany Trang et al., *Experts say scale of Change cyberattack shows risk of centralized claims processing*, STAT+ (Feb. 27, 2024), https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-consolidation-risks/.

[30] *See* Darius Tahir et al., *Health Industry Struggles to recover from cyberattack on a unit of UnitedHealth*, https://wamu.org/story/24/03/09/health-industry-struggles-to-recover-from-cyberattack-on-a-unit-of-unitedhealth/

[31] *Id.*

[32] *See* Richard J. Pollack, *AHA Urges More Congressional Action to Help Providers Affected By Change Healthcare Cyberattack*, AMERICAN HOSPITAL ASSOCIATION (Mar. 13, 2024), https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack.

73. Just weeks after the outage, the AHA conducted a survey of over 1,000 providers, reporting that "74% reported direct patient care impact, including delays in authorizations for medically necessary care."[33] Further, the AHA reported the results of its survey:

> [H]ospitals, health systems and other providers are experiencing extraordinary reductions in cash flow, threatening their ability to make payroll and to acquire the medical supplies needed to provide care. In the same survey, 94% of hospitals reported that the Change Healthcare cyberattack was impacting them financially, with more than half reporting the impact as "significant or serious." Indeed, a third of the survey respondents indicated that the attack has disrupted more than half of their revenue. The urgency of this matter grows by the day.[34]

74. Another survey of Massachusetts healthcare providers reported that costs from the outage, just in Massachusetts, ranged from $1 million a day for a single community hospital to $12 million a day for a single health system.[35] Other analysts estimated, in mid-March, that providers were losing between $500 million and $1 billion in daily revenue compared with 2023.

75. To make matters worse, on March 18, 2024, ratings agency Fitch said that certain healthcare providers that use its services may see a hit to their credit profile because of the Data Breach's impact on cash flows.[36]

---

[33] *Id.*
[34] *See id.*
[35] *See* Alison Kuznitz, *Mass. hospitals feeling fiscal pinch from Change Healthcare cyber* breach, WBUR (Mar. 12, 2024), https://www.wbur.org/news/2024/03/12/change-healthcare-cyber-attack-massachusetts.
[36] *See UnitedHealth unit hack may hit pharmacies, providers' credit profiles, Fitch says*, REUTERS (Mar. 18, 2024, 7:58 AM), https://www.reuters.com/business/healthcare-pharmaceuticals/fitch-says-unitedhealth-unit-hack-could-hit-smaller-pharmacies-care-providers-2024-03-18/.

76. The AHA sought help from the federal government, noting that "[t]he urgency of this matter grows by the day." The federal government provided some partial relief on March 9, 2024, making available "accelerated payments" to advance funds for certain Medicare claims.[37] UHG also implemented a bridge loan program in early March, offering interest-free loans for a fraction of the total payments outstanding, initially with onerous rates and terms such as a five-day repayment requirement upon notice; the ability for UHG's bank to recoup funds "immediately and without prior notification[;]" and a requirement that providers give UHG and its subsidiaries "access to past, current, and future claims payment data[.]"[38] Providers widely report that these programs fall far short of addressing their needs. Some providers also reported that they felt pressured by UHG to make positive public statements about its programs.[39] According to one provider, Emily Benson, she received emails and voicemails from Optum's communication department

[37] *See Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments*, CENTERS FOR MEDICARE & MEDICAID SERVICES (Mar. 9, 2024), https://www.cms.gov/newsroom/fact-sheets/change-healthcare/optum-payment-disruption-chopd-accelerated-payments-part-providers-and-advance.

[38] *See UnitedHealth offers over $3.3 bln in loans to providers hit by attack on unit*, REUTERS (Mar. 28, 2024), https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-group-has-paid-over-33-bln-care-providers-hit-by-cyberattacks-2024-03-28/; *AHA Expresses Concerns with UHG Program in Response to Cyberattack on Change Healthcare*, AMERICAN HOSPITAL ASSOCIATION (Mar. 4, 2024), https://www.aha.org/lettercomment/2024-03-04-aha-expresses-concerns-uhg-program-response-cyberattack-change-healthcare.

[39] *See UnitedHealth Grapples With Communications During Hack Crisis*, WSJ (April 3, 2024), https://www.wsj.com/articles/unitedhealth-grapples-with-communications-during-hack-crisis-b1dfccd8.

requesting that she go on social media or talk to journalists and make statements about the help she received from UHG.[40]

77. On or around March 22, 2024—only after imposing a total shutdown on the industry for a full month—did UHG begin to restore some of Change's systems and to process some of the backlog in payments. By that time, a backlog of unpaid claims had accumulated—not including claims from the past month that providers could not submit for payment—which totaled over $14 billion.[41]

78. Restoration and repayment still are nowhere near complete. Providers, including Plaintiffs, are still struggling to manage their businesses without a substantial portion of their earned revenues. A survey of physician practices by the American Medical Association found that, from April 19 – April 24, 2024, 85% continued to experience disruptions in claim payments, 79% still could not receive electronic remittance advice, 75% reported barriers with claim submission, and 60% faced challenges in verifying patient eligibility.[42] Moreover, the survey showed that 55% of practitioners had to use their personal funds, and 31% reported they could not make payroll.

79. On April 25, 2024, a coalition of 21 state attorneys general sent a letter to UHG demanding more meaningful action to better protect providers, pharmacies, and

---

[40] *Id.*

[41] *UnitedHealth Unit Will Start Processing $14 Billion Medical Claims Backlog After Hack*, REUTERS (Mar. 22, 2024), https://www.reuters.com/technology/cybersecurity/unitedhealth-says-several-services-handling-medical-claims-unit-change-will-go-2024-03-22/.

[42] *See* American Medical Association, *Change Healthcare cyberattack impact* (April 29, 2024), https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf.

patients harmed by the outage, noting that providers in all 21 states were reporting "catastrophic billing and payment backlogs, and other problems stemming from the extended breakdown of Change Healthcare," and "both Change Healthcare's and UnitedHealth Group's responses to the crisis have been inadequate."[43] At a Senate hearing on May 1, 2024, Sen. Marsha Blackburn, R-Tenn., criticized UHG's recovery effort saying that she has been "absolutely inundated" by providers and patients who are still struggling to get reimbursed and to get clarity about the incident. Many providers have had to take out emergency loans at high interest rates, and dip into personal savings accounts, among other things.

D. Defendants Had Notice of the Foreseeable Data Breach and Resulting Shutdown

80. BlackCat was essentially able to walk right into Change's internal networks; nothing about BlackCat's challenge to Change's cybersecurity was extraordinary. Setting aside the FBI's specific advisory and recommended mitigation measures for this specific cybercriminal group (repeated and re-publicized after 2022 by other government organizations[44]), companies know that passwords and other login credentials are widely compromised and that they need to be prepared for cyberattacks. Cybercriminals target the

[43] *See* Letter from Attorneys General, *Re: Change Healthcare Disruptions* (Apr. 25, 2024), https://oag.ca.gov/system/files/attachments/press-docs/4.25.24%20Letter%20to%20UnitedHealth%20Group%20CEO%20Andrew%20Witty%20re%20Change%20Healthcare%20Disruptions%5B1%5D.pdf.

[44] *See e.g. Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, UNITED STATES DEPARTMENT OF JUSTICE (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

healthcare industry at a higher rate due to the treasure trove of confidential health and personal information maintained and stored by healthcare organizations. In 2023 alone, the FBI reported 249 ransomware attacks in the healthcare industry.[45]

81. Cyberattacks against the healthcare industry in particular have been common for over a decade, with the FBI warning as early as 2011 that cybercriminals targeting healthcare providers and others were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII.[46] The FBI again warned healthcare stakeholders in 2014 that they are the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[47]

82. In 2017, the Department of Health and Human Services released a ransomware fact sheet. This document clearly explained to entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") that "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has

[45] *See* Darius Tahir et al., *Health industry struggles to recover from cyberattack on a unit of UnitedHealth*, NPR (Mar. 9, 2024, 7:00 AM), https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united.

[46] Gordon M. Snow, FBI, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (Sept. 14, 2011).

[47] *See FBI Cyber Bulletin: Malicious Actors Targeting Protected Health Information*, Public Intelligence (Aug. 19, 2014), https://publicintelligence.net/fbi-targeting-healthcare/.

occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."[48]

83. Then, in January 2023, the Department of Health and Human Service's Office of Information Security and Healthsector Cybersecurity Coordination Center, issued a publication warning to the health sector specifically it about BlackCat titled, "Royal & BlackCat Ransomware: The Threat to the Health Sector."[49] HHS reported that BlackCat is "focused on the U.S. . . . [including]healthcare[.]"[50] HHS also reprinted the FBI's laundry list of defenses, including the use of multifactor authentication.[51]

84. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into healthcare networks for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of five hundred or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[52]

---

[48] *See Fact Sheet: Ransomware and HIPAA,* U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Sept. 20, 2021), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html.
[49] *See Royal & BlackCat Ransomware: The Threat to the Health Sector,* HHS, https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202&_ga=2.232273750.877001956.1718600643-1694382590.1718600639
[50] *Id.*
[51] *Id.*
[52] *Editorial: Why Do Criminals Target Medical Records,* THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

85. This is not the first time that the UHG conglomerate has dealt with a data breach. In May 2023, United Healthcare, a UHG subsidiary, had to notify members that PHI may have been compromised due to a credential stuffing attack that occurred on the United Healthcare mobile app in February 2023.[53]

86. BlackCat, specifically, has a reputation for engaging in "double extortion tactics," that is, exfiltrating confidential and sensitive data before using ransomware to encrypt the files.

87. Accordingly, Defendants knew, given the vast amount of PHI and PII that healthcare providers such as Plaintiffs and Class members acquire and transmit to Defendants directly or through vendors and that in turn, Defendants store and maintain, that they were a target for cybercriminals and should have taken all reasonable measures to avoid cyberattacks. Defendants also understood the risks posed by their insecure data security practices and computer networks. Instead, in June 2023, UHG elevated an individual, Steven Martin, to the position of UHG's chief information security officer even though Mr. Martin had had not previously worked in a full-time cybersecurity role in his career. The Audit and Finance committee of UHG's board, which has responsibility for overseeing cybersecurity risk to the company, was also composed of individuals with no meaningful cybersecurity expertise.[54] Defendants' failure to heed warnings and failure to

[53] *See Credential Stuffing Attack Exposed United HealthCare Member Data*, THE HIPAA JOURNAL (May 2, 2023), https://www.hipaajournal.com/credential-stuffing-attack-exposed-united-healthcare-member-data/.
[54] *See* Letter from Senator Ron Wyden to Federal Trade Commission and Securities and Exchange Commission (May 30, 2024),

adequately maintain their computer networks secure resulted in the shutdown and harm to Plaintiffs and Class members.

E. Defendants' Duties to Plaintiffs and Class Members

88. Defendants marketed and sold their services to Plaintiffs and Class members, directly and indirectly, and were aware, at all relevant times, that healthcare providers such as Plaintiffs and Class members handle PHI and PII on a daily basis and that they are required by law to keep such data confidential. Thus, Defendants were also required by law, and owed Plaintiffs and Class members a duty, to properly secure their computer networks and encrypt and maintain PHI and PII using industry standard methods, utilize available technology to defend their computer networks from invasion, to enforce appropriate policies and maintain competent staffing for cybersecurity matters, to maintain an appropriate incident response measures, including a business continuity plan, and otherwise to act reasonably to prevent foreseeable harms, among other things.

89. Defendants' duties to Plaintiff and the Class, including the duty to use reasonable security measures, maintain appropriate incident response measures and a business continuity plan, also arose from the special relationship that existed between them, on the one hand, and Plaintiffs and Class members, on the other hand. The special relationship arose because Plaintiffs and the members of the Class entrusted Defendants (or their partners who entrusted Defendants) with PHI and PII. Independent of this special relationship, Defendants also owed a common law duty to safeguard their computer

---

https://www.finance.senate.gov/imo/media/doc/wyden_letter_to_ftc_and_sec_on_uhg_cybersecuritypdf.pdf

networks and the data in their possession from foreseeable attack, and to minimize the foreseeable impact of any such attack on Plaintiffs and Class members. These duties arose because each of Defendants had knowledge of the threat and the resources necessary to protect their computer networks, including from BlackCat, but neglected to adequately invest in security measures, despite their obligations to protect such information. Accordingly, Defendants breach their common law, statutory and other duties to Plaintiffs and Class members.

90. Defendants' duties to, among other things, use reasonable security measures also arose under HIPAA. As a healthcare company, and by handling medical patient data, Defendants are covered entities under HIPAA (45 C.F.R. § 160.103), and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

91. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information that is kept or transferred in electronic form. HIPAA-covered entities must implement

safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

92. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendants. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and, implement policies to correct any security problems.[55] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach. [56]

F. Defendants Breached their Legal Duties to Plaintiffs

93. Defendants breached their duties to Plaintiffs and the Class at every turn, utterly failing in their obligations to implement basic industry standard cybersecurity

[55] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[56] *Id.*

measures for uniquely sensitive and valuable data entrusted to them, and by worsening the impact of the Data Breach on the Class and on society as a whole.

94. Defendants breached their duties to Plaintiffs and the Class, including by inadequately protecting against criminal ingress into their systems given the known sophistication of hackers and their interest in healthcare data. Multifactor authentication ("MFA") is a very basic yet effective security measure that ordinary consumers use in the ordinary course, to access portals to information that poses a risk of harm if it falls into the wrong hands. MFA would be a basic expectation for a company handling the breadth and sensitivity of the information that flows through Change's systems. Consistent with the FBI's advisements to use MFA to block entry by BlackCat, the Federal Cybersecurity & Infrastructure Security Agency (CISA) has also explained, in a 2022 bulletin, that MFA is important to protect Internet-facing portals (such as Change's Citrix portal), because "[a]dversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries."[57] In June 2023, the U.S. Department for Health & Human Services echoed the same warnings in a newsletter issued for the healthcare industry specifically, explaining

[57] *Multi-Factor Authentication Fact Sheet*, CISA (Jan. 2022), https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf (emphasis added, footnote omitted).

that: "Weak or non-existent authentication processes leave your digital door open to intrusion by malicious actors and increase the likelihood of potential compromise of sensitive information – including electronic protected health information (ePHI). Robust authentication serves as the first line of defense against malicious intrusions and attacks, yet a recent analysis of cyber breaches reported that 86% of attacks to access an organization's Internet-facing systems (e.g., web servers, email servers) used stolen or compromised credentials."[58]

95. Defendants also breached their duties by failing to adequately monitor their computer networks, which allowed hackers to roam and forage within Change's systems for nine days without detection. Monitoring a network for suspicious activity—such as unusual database access, changes in access patterns by the particular user whose credentials were employed, configuration changes to files, new software installations, and traffic from unexpected or unusual sources—is a basic cybersecurity precaution. It is extremely unlikely that the individual whose login credentials were compromised and obtained by BlackCat had a legitimate need to access, let alone download, files associated with dozens of distinct healthcare entities *and* source code files within a nine-day time span, *and* to access the systems that the hackers ultimately encrypted. Basic monitoring would also have alerted Defendants of the extensive suspicious activities that were occurring from a new IP

[58] *See June 2023 OCR Cybersecurity Newsletter*, US DEPARTMENT OF HEALTH AND HUMAN SERVICES (Jun. 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html.

address or device (or several), yet it appears there were no red flags when all these activities occurred.

96. Defendants breached their duties by failing to wall systems off from individuals who could not conceivably need to access them; as the FBI put it, failing to "configure access controls," and "[i]mplement network segmentation."[59] This is evident in the scope and expansiveness of the exfiltrated data, as well as that the hackers were able to access, via a public-facing Citrix portal, Change's internal backup systems which would not ordinarily be required in the performance of any employee's routine job functions.

97. Defendants breached their duties by failing to control and limit the ability of a single individual to make changes to the configuration of internal systems, such as mandating administrator credentials to install software consistent with guidance from the FBI. This is evidenced by the fact that with nothing more than Citrix login credentials, BlackCat was able to encrypt Change's systems and prevent Defendants from gaining access.

98. Defendants breached their duties by failing to plan for a foreseeable ransomware attack and having a business continuity plan in place; instead, Defendants wreaked havoc on providers and the healthcare industry by shutting down critical services without warning. Defendants did not "[i]mplement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location," and they did not "[e]nsure copies of critical data are not

[59] *See BlackCat/ALPHV Ransomware Indicators of Compromise*, FBI CYBER DIVISION (Apr. 19, 2022), https://www.ic3.gov/Media/News/2022/220420.pdf.

accessible for modification or deletion from the system where the data resides,"[60] as evidenced by the fact that hackers encrypted all available copies and backups through a Citrix portal.

99. Defendants breached their duties by withholding important information from providers, including an accurate timeline for system restoration, which compounded and aggravated the immense challenges healthcare providers already faced when their administrative processes were curtailed, and revenues cut off. Defendants also failed to promptly disclose the cause of the outage, the extent to which Change's systems had been compromised, or the critically important fact, known to Defendants, that services would not be promptly restored, and reimbursements owed to providers would not promptly be made. Even as of the date of this filing, Defendants still have not provided conclusive information regarding a return to full functionality for Change services, or when remittances due to providers will finally be made current, if at all.

100. Through at least all the actions and inactions above, Defendants breached their obligations to Plaintiffs and Class members and/or were otherwise negligent and reckless. On information and belief, and as discussed above, Defendants failed to meet the minimum standards under HIPAA, Section 5 of the FTC Act, and all of the following established standards in reasonable cybersecurity readiness: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-

[60] *See id.*

1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC).

G. Plaintiffs' Experiences

Alabama Plaintiff

101. Plaintiff **Alabama Family Foot Clinic, PC** ("Foot Clinic") is a licensed healthcare provider serving patients in Rainbow City, Alabama.

102. Plaintiff Foot Clinic contracts with FlexMedical, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

103. FlexMedical, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff Foot Clinic submit their claims to FlexMedical, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff Foot Clinic.

104. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Foot Clinic could no longer submit claims through FlexMedical and obtain payments for those claims. After the shutdown began and for several weeks thereafter, Plaintiff Foot Clinic was not paid for any claims despite continuing to treat patients. Plaintiff Foot Clinic has only recently started to get payments from using a new billing system, but a number of submitted claims still remain to be paid, while Plaintiff continues to treat patients. Plaintiff Foot Clinic relies on the payments it

receives from submitted claims to pay basic business expenses, including salaries and wages to employees, other associated business expenses, and to further grow the practice.

105. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Foot Clinic's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff Foot Clinic has also had to contract with another vendor to submit claims, which has increased Plaintiff Foot Clinic's administrative costs.

Arizona Plaintiffs

106. Plaintiff **Desert ABA Solutions LLC** ("Desert") is a licensed healthcare provider serving patients in Yuma, Arizona.

107. Plaintiff Desert contracts with Central Reach Essentials, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

108. Central Reach Essentials, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff Desert submit their claims to Central Reach Essentials, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff Desert.

109. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Desert could no longer submit claims through Central Reach Essentials and obtain payments for those claims. After the shutdown and for several

weeks thereafter, Plaintiff Desert was not paid for any claims despite continuing to treat patients. Plaintiff Desert relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees, other associated business expenses, and to further grow the practice.

110. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Desert's owner has had to take out funds from her personal savings account and maxed out a credit card to meet payroll and pay other basic expenses. Plaintiff Desert's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff Desert has also had to contract with another vendor to submit claims, which has increased Plaintiff Desert's administrative costs.

111. Plaintiff **Unique Integrated Care** ("UIC") is a licensed healthcare provider serving patients in Tempe, Arizona.

112. Plaintiff UIC contracts with Valant, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

113. Valant, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff UIC submit their claims to Valant, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff UIC.

114. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff UIC could no longer submit claims through Valant and obtain payments for those claims. After the shutdown and for several weeks thereafter, Plaintiff UIC was not paid for any claims despite continuing to treat patients. Plaintiff UIC relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

115. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff UIC's owner had to take out personal funds to meet payroll and pay other basic expenses. Plaintiff UIC's staff resources were also diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

116. On March 22, 2024, Plaintiff UIC had to close its business.

California Plaintiffs

117. Plaintiff **Riverbend Counseling Services** ("Riverbend") is a licensed healthcare provider serving patients in Sacramento, California.

118. Plaintiff Riverbend contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

119. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff Riverbend submit their claims to Therapy Notes, which in turn uses Change

Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff Riverbend.

120. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Riverbend could no longer submit claims through Therapy Notes and obtain payments for those claims. After the shutdown began and for several weeks thereafter, Plaintiff Riverbend was only paid partially for its claims despite continuing to treat patients. Plaintiff Riverbend relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to Plaintiff Riverbend's owner.

121. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Riverbend has had to take out funds reserved for paying quarterly taxes to meet payroll and pay other basic expenses. Plaintiff Riverbend's owner has also diverted his time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff Riverbend also had to temporarily utilize another vendor to submit claims.

122. Plaintiff **E5 Therapy** ("E5") is a licensed healthcare provider serving Veterans, Military members, and their family members, in California and Florida.

123. Plaintiff E5 contracted with Sessions Health, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

124. Sessions Health, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare

providers such as Plaintiff E5 submit their claims to Sessions Health, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff E5.

125. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff E5 could no longer submit claims through Sessions Health and obtain payments for those claims. After the shutdown and for several weeks thereafter, Plaintiff E5 was not paid for any claims despite continuing to treat patients. After switching to two new clearinghouses to submit claims to get paid, Plaintiff began to receive payments for billing. E5 relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees, and to further grow the practice, including hiring additional therapists to treat patients.

126. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff E5 had to take out a $100,000 line of credit, which E5's owner had to personally guarantee, to meet payroll and pay other basic expenses. Plaintiff E5's staff resources have also been diverted to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks, including sorting through all the backed billing to ensure proper compensation and to make sure they have not lost any money.

Colorado Plaintiff

127. Plaintiff **KidStuff Child and Family Counseling PC** ("KidStuff") is a licensed healthcare provider serving patients in the following cities in Colorado: Loveland, Greeley, Fort Collins, Longmont, Westminster, Durango, Grand Junction, and Colorado Springs.

128. Plaintiff KidStuff contracted with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

129. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff KidStuff submit their claims to Therapy Notes, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff KidStuff.

130. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff KidStuff could no longer submit claims through Therapy Notes and obtain payments for those claims. Since the shutdown, Plaintiff KidStuff has not fully recovered with the pace and number of claims being paid prior to the shutdown. For approximately four weeks following the shutdown, Plaintiff KidStuff did not receive any electronic claims payments. For approximately four weeks after that, Plaintiff KidStuff received delayed payments, and Plaintiff KidStuff had been unable to recover a financial balance equal to the financial balance prior to the shutdown due to the high interest loans acquired in the first four weeks when there were no payments coming in to pay expenses. Plaintiff KidStuff relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees, and to further grow the practice, including hiring additional therapists to treat patients.

131. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff KidStuff has had to take out emergency loans with interest totaling

almost $30,000 to meet payroll and pay other basic expenses. Plaintiff KidStuff's staff resources have also been diverted to resolving the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff KidStuff also had to contract with another vendor to replace Therapy Notes, which has increased Plaintiff KidStuff's administrative costs.

Florida Plaintiffs

132. Plaintiff **Urological Consultants of Florida** ("Urological") is a licensed healthcare provider serving patients in the greater Miami region in Florida.

133. Plaintiff Urological contracts with Advanced Data Systems Corporation ("ADS"), which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

134. ADS, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff Urological submit their claims to ADS, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff Urological.

135. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Urological could no longer submit claims through ADS and obtain payments for those claims. After the shutdown began and for several weeks thereafter, Plaintiff Urological, despite continuing to treat patients, was not paid for any claims submitted. Plaintiff Urological had to switch to a different vendor to submit claims

for payment. Plaintiff Urological relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to himself and employees.

136. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Urological has had to dip into his emergency fund to meet payroll and pay other basic expenses. Plaintiff Urological's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Additionally, the change to another vendor also increased Plaintiff Urological's administrative costs.

137. Plaintiff **Ball's Rexall Drugs, Inc., D/B/A B&W Rexall Drugs** ("B&W") is a pharmacy serving patients in Inverness, Florida, as well as the surrounding communities of Hernando, Floral City, Lecanto, Crystal River, Homosassa, Wildwood, Lake Panasoffkee, Bushnell, and The Villages, since 1989.

138. Plaintiff B&W contracted with Change Healthcare to process insurance claims and pharmaceutical manufacturer coupons.

139. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff B&W could no longer submit claims or savings cards/coupons through Change Healthcare and obtain payments for those claims. After the shutdown began and for weeks thereafter, Plaintiff B&W had to find an alternative way to submit and resubmit claims and savings cards/coupons to obtain payments. Plaintiff B&W has been paid only about $2,000, a small fraction of its usual earnings. Plaintiff B&W relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

140. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff B&W's owner had to withdraw money from his personal accounts and retirement funds to meet payroll and pay other basic expenses. Plaintiff B&W's staff resources have also been diverted to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

Illinois Plaintiff

141. Plaintiff **Cloe Chiropractic Center** ("Cloe") is a licensed healthcare provider serving patients in Mount Vernon, Illinois.

142. Plaintiff Cloe contracts with EZBIS, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

143. EZBIS, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff Cloe submit their claims to EZBIS, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff Cloe.

144. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Cloe could no longer submit claims through EZBIS and obtain payments for those claims. After the shutdown and for several weeks thereafter, Plaintiff Cloe was not paid for any claims despite continuing to treat patients. Plaintiff Cloe relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to himself and his office manager.

145. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Cloe's owner has had to take out funds from his personal accounts to meet payroll and pay other basic expenses. Plaintiff Cloe's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff Cloe has also had to contract with another vendor to replace EZBIS, which has increased Plaintiff Cloe's administrative costs.

Indiana Plaintiff

146. Plaintiff **Mind Garden, LLC** ("Mind Garden)" is a licensed healthcare provider serving patients in Indianapolis, Indiana.

147. Plaintiff Mind Garden contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

148. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

149. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Mind Garden could no longer submit claims through Therapy Notes and obtain payments for those claims. After the shutdown, Plaintiff Mind Garden was not paid for any claims despite continuing to treat patients. Plaintiff Mind Garden relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to Plaintiff Mind Garden's owner and a biller.

150. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Mind Garden's owner has also diverted her time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff Mind Garden has also had to switch to a different vendor to submit claims, which has increased Plaintiff Mind Garden's administrative costs.

Iowa Plaintiff

151. Plaintiff **Serenity Therapy, LLC** ("Serenity") is a licensed healthcare provider serving patients in Iowa, Illinois, and Wisconsin.

152. Plaintiff Serenity submits insurance claims through Health Choices and Dean Health Plan ("Dean"). Health Choices uses Change Healthcare to process insurance claims submitted by its providers, among other things. Dean uses a third-party program to receive claims but uses Change Healthcare to pay claims. Healthcare providers such as Plaintiff Serenity submit their claims to Health Choices, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff Serenity; and/or, submit their claims to Dean, which in turn uses Change Healthcare to pay claims.

153. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Serenity could no longer submit claims through Health Choices and obtain payments for those claims. While Plaintiff Serenity was able to submit claims through Dean, Plaintiff Serenity could not obtain payments for those claims. Approximately seven weeks after the shutdown, Plaintiff Serenity started receiving payments for claims submitted through Dean because Dean stopped using Change

Healthcare. Plaintiff Serenity, however, is still waiting to receive payments for claims submitted through Health Choices, despite continuing to treat patients. Plaintiff Serenity relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to herself.

154. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Serenity has had to withdraw from reserves saved for paying taxes to meet payroll and pay other basic expenses. Plaintiff has also diverted time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff Serenity has also had to purchase special forms to submit paper claims, which has increased Plaintiff Serenity's administrative costs.

Kansas Plaintiff

155. Plaintiff **Pittsburg Internal Medicine PA** ("PIM") is a licensed healthcare provider serving patients in Pittsburg, Kansas.

156. Plaintiff PIM contracted with Change Healthcare to process insurance claims and verify insurance.

157. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff PIM could no longer submit claims, verify insurance through Change Healthcare, and obtain payments for those claims. After the shutdown and for some time thereafter, Plaintiff PIM was not paid for any claims despite continuing to treat patients. Plaintiff PIM relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

158. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff PIM has had to take out a line of credit of $50,000, and PIM's owner has had to take out funds from her personal accounts to meet payroll and pay other basic expenses. Plaintiff PIM's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks, including assisting patients with finding alternative medicines because patients were unable to use their copay cards through Defendants' computer networks. Plaintiff PIM has also had to contract with another vendor to replace Change Healthcare, which has increased Plaintiff PIM's administrative costs.

Maryland Plaintiff

159. Plaintiff **Gievers-Zuniga Foot & Ankle Center** ("GZFA") is a licensed healthcare provider serving patients in Olney, Maryland.

160. Plaintiff GZFA's biller used OmniMD, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

161. OmniMD, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff GZFA submit their claims to OmniMD, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff GFZA.

162. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff GZFA could no longer submit claims through OmniMD

and obtain payments for those claims. After the shutdown began and for several weeks thereafter, Plaintiff GZFA was not paid for any claims despite continuing to treat patients. Only after switching to a different clearinghouse on April 12, 2024, did Plaintiff GZFA start to receive payments. Plaintiff GZFA relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to herself and her biller, among other business associated expenses.

163. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff GZFA had to take out a new credit card with a $25,000 limit, applied for a line of credit of $50,000, and Plaintiff GZFA's owner has had to exhaust her personal savings, to meet payroll and pay other basic expenses. Plaintiff GZFA's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. As a result of the Data Breach, Plaintiff GZFA has had to pay $500 to switch to TriZetto, a different clearinghouse, to submit claims through OmniMD, which has increased Plaintiff GZFA's administrative costs.

Massachusetts Plaintiff

164. Plaintiff **Kajal Gehi Psychotherapy, LLC** ("KGP") is a licensed healthcare provider serving patients throughout the state of Massachusetts.

165. Plaintiff KGP contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

166. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

167. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff KGP could no longer submit claims through Therapy Notes and obtain payments for those claims. After the shutdown began and for several weeks thereafter, Plaintiff KGP, despite continuing to treat patients, was not paid for any claims submitted. Plaintiff KGP had to switch to a different vendor to submit claims for any of its claims to be paid. Plaintiff KGP relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to herself.

168. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff KGP has diverted her time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

Michigan Plaintiff

169. Plaintiff **Irwin Counseling Service, PLLC** ("ICS") is a licensed healthcare provider serving patients in Jackson, Michigan.

170. Plaintiff ICS contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

171. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

172. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff ICS could no longer submit claims through Therapy Notes and obtain payments for those claims. After the shutdown, Plaintiff ICS was not paid for any claims despite continuing to treat patients. Plaintiff ICS relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees, and to further grow the practice, including hiring additional therapists to treat patients.

173. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff ICS's owner has had to withdraw money from his personal funds to meet payroll and pay other basic expenses. Plaintiff ICS's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff ICS has also had to contract with another vendor to replace Therapy Notes, which has increased Plaintiff ICS's administrative costs.

Minnesota Plaintiff

174. Plaintiff Lake Acupuncture LLC ("Lake") is a licensed healthcare provider serving patients in Minneapolis, Minnesota.

175. Plaintiff Lake contracts with Office Ally, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

176. Office Ally, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

177. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Lake could no longer obtain payments for claims submitted through Office Ally. After the shutdown began, despite continuing to treat patients, Plaintiff Lake was able to submit claims but not able to receive payments for many of those claims because they were through insurers that use Defendants' computer networks for processing payments, among other things. At or around the beginning of April, Plaintiff Lake received some backlogged payments, however, there have been continued delays. Office Ally had to find alternative ways to submit Plaintiff Lake's claims for payment. Plaintiff Lake relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees, among other business associated expenses.

178. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Lake's owner has had to take out funds from his business savings account to meet payroll and pay other basic expenses. Plaintiff Lake's owner has also diverted his time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

Mississippi Plaintiff

179. Plaintiff **Diabetes & Endocrine Institute** ("DEI") is a licensed healthcare provider serving patients in Flowood, Mississippi.

180. Plaintiff DEI contracts with Medisoft, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

181. Medisoft, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

182. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff DEI could no longer submit claims through Medisoft and obtain payments for those claims. After the shutdown began and for approximately three months thereafter, Plaintiff DEI was not paid for any claims despite continuing to treat patients. After upgrading to a version of Medisoft that accepts a different clearinghouse, Plaintiff DEI has only recently started to receive payments, but there remain an outstanding number of unpaid claims. Plaintiff DEI relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

183. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff DEI's owner and his wife have had to take out personal loans and cash out their retirement funds to meet payroll and pay other basic expenses, and to keep DEI's practice open. Plaintiff DEI's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks, including finding alternative ways to submit and resubmit claims to obtain payments. Plaintiff DEI has also had to fill out paper claims and mail them to Medicare, which takes longer. Plaintiff DEI has also had to upgrade his Medisoft program to use a different clearinghouse, which has increased Plaintiff DEI's administrative costs.

Missouri Plaintiff

184. Plaintiff **South City Counseling STL** ("South City") is a licensed healthcare provider serving patients in St. Louis, Missouri.

185. Plaintiff South City contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

186. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Plaintiff South City has been informed that Therapy Notes no longer uses Change Healthcare.

187. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff South City could no longer submit claims through Therapy Notes and obtain payments for those claims. After the shutdown began and for approximately several weeks thereafter, Plaintiff South City, despite continuing to treat patients, was not paid for any claims submitted. Plaintiff South City relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to Plaintiff South City's owner.

188. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff South City has had to rely exclusively on its business AMEX credit card to pay basic business expenses, and other associated business expenses. Plaintiff South City's owner has also diverted her time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

New Jersey Plaintiffs

189. Plaintiff **Nancy Fish LCSW, MPH** ("Fish") is a licensed healthcare provider serving patients in Bergen County, New Jersey.

190. Plaintiff Fish contracts with Apex, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

191. Apex, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

192. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Fish could no longer submit claims through Apex and obtain payments for those claims. After the shutdown and for several weeks thereafter, Plaintiff Fish had to find alternative ways to submit and resubmit claims to obtain payments and to continue to treat patients. Plaintiff Fish relies on the payments she receives from submitted claims to pay basic business expenses.

193. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Fish has diverted her time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

194. Plaintiff **Serenity Counseling Center NJ LLC** ("SCC") is a licensed healthcare provider serving patients in Freehold Township, New Jersey.

195. Plaintiff SCC contracts with SimplePractice, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

196. SimplePractice, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

197. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff SCC could no longer submit claims through SimplePractice and obtain payments for those claims. Since the shutdown, Plaintiff SCC has had to find alternative ways to submit and resubmit claims to obtain payments and to continue to treat patients. Plaintiff SCC relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

198. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff SCC's owner has had to withdraw money from her personal and retirement accounts to meet payroll and pay other basic expenses. Plaintiff SCC's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff SCC has also had to submit claims through different clearinghouses to try to get paid for services provided, which has increased Plaintiff SCC's administrative costs.

New Mexico Plaintiff

199. Plaintiff **Robert Mullan, DPM, Inc.** ("Mullan") is a licensed healthcare provider serving patients in Las Cruces, New Mexico.

200. Plaintiff Mullan contracts with CompuLink, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

201. CompuLink, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

202. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Mullan could no longer submit claims through CompuLink and obtain payments for those claims. After the shutdown, Plaintiff Mullan was not paid for any claims despite continuing to treat patients, resulting in total losses at approximately $128,000. Plaintiff Mullan relies on the payments he receives from submitted claims to pay basic business expenses, including salaries and wages to himself and employees.

203. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Mullan has had to take out funds from his own personal account to meet payroll and pay other basic expenses; furlough seven out of ten employees; and, has had to reduce his hours for treating patients. Plaintiff Mullan's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff Mullan has also had to contract with another vendor to replace CompuLink, which has increased Plaintiff Mullan's administrative costs.

New York Plaintiff

204. Plaintiff **With Grace Mental Health Counseling PLLC** ("WGMHC") is a licensed healthcare provider serving patients in New York, including in Clifton Park, Saratoga Springs, and Queensbury.

205. Plaintiff WGMHC contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

206. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

207. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff WGMHC could no longer submit claims through Therapy Notes and obtain payments for those claims. Since the shutdown, Plaintiff WGMHC received some payments for claims that were billed prior to the Data Breach, however, Plaintiff WGMHC could not bill out new claims electronically resulting in delays in payments for those claims, despite continuing to treat patients. Plaintiff WGMHC relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

208. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff WGMHC's owners had to take out a business loan with an interest rate of 9.5% to meet payroll and pay other basic expenses. Plaintiff WGMHC's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

North Carolina Plaintiff

209. Plaintiff **Anew U Counseling Services, PLLC** ("Anew") is a licensed healthcare provider serving patients in Raleigh, North Carolina and Waxhaw, North Carolina.

210. Plaintiff Anew contracts with TheraNest, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

211. TheraNest, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

212. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Anew could no longer submit claims through TheraNest and obtain payments for those claims. After the shutdown began and for weeks thereafter, Plaintiff Anew had to resort to manually submitting claims to each insurance payer to obtain payments; this manual submission process persisted for some time and caused significant delays in receiving payments. Furthermore, Plaintiff Anew had to process payment postings manually. Plaintiff Anew relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

213. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Anew has had to take out emergency loans with interest rates of 11% to meet payroll and pay other basic expenses. Plaintiff Anew's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow

problems caused by the shutdown of Defendants' computer networks, including hiring two part-time employees to handle the manual faxing of claims and posting of insurance payments.

Ohio Plaintiffs

214. Plaintiff **Cultivating Mind LLC** ("CM") is a licensed healthcare provider serving patients in the state of Ohio.

215. Plaintiff CM contracts with Tebra, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

216. Tebra, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

217. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff CM could no longer submit claims through Tebra and obtain payments for those claims. After the shutdown and for approximately 12 weeks thereafter, Plaintiff CM only received $5,220.00 for claims submitted prior to the Data Breach, despite continuing to treat patients. Plaintiff CM relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

218. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff CM's owner has had to use personal funds to meet payroll and pay other basic expenses and has had to use personal credit cards to pay basic expenses. Plaintiff CM's staff resources have also been diverted from treating patients at full capacity to trying

to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

219. Plaintiff **The Wellife, LLC** ("The Wellife") is a licensed healthcare provider serving patients in North Canton, Ohio.

220. Plaintiff The Wellife contracts with SimplePractice, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

221. SimplePractice, in turn, partners with Change Healthcare, among other clearinghouses, to process insurance claims submitted by its clients, among other things.

222. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff The Wellife could submit claims through SimplePractice, but SimplePractice noted that because of the Data Breach, Plaintiff The Wellife's claims were unlikely to be picked up by the insurance processors on the other end. Therefore, claims submitted after February 21, 2024, were not processed for payment by many insurance companies that Plaintiff The Wellife contracts with. After the shutdown began and for approximately a month thereafter, Plaintiff The Wellife was not paid for any claims despite continuing to treat patients and continues to wait for payments from one insurance company. Plaintiff The Wellife relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees and three contractors.

223. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff The Wellife's staff resources have also been diverted from treating

patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

Pennsylvania Plaintiffs

224. Plaintiff **Kaitlin Heckman LLC** ("Heckman") is a licensed healthcare provider serving patients in Pittsburgh, Pennsylvania and Uniontown, Pennsylvania.

225. Plaintiff Heckman contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

226. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

227. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Heckman could no longer submit claims through Therapy Notes and obtain payments for those claims. Since the shutdown, Plaintiff Heckman has had to find alternative ways to submit and resubmit claims, including submitting paper claims and switching to a new billing platform, to obtain payments and to continue to treat patients. Plaintiff Heckman relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to its owner and contractor.

228. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Heckman has had to take out personal funds to meet payroll and pay other basic expenses. Plaintiff Heckman's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the

shutdown of Defendants' computer networks, including devoting time to navigating alternative systems to Therapy Notes to receive payment.

229. Plaintiff **Rebecca Williams, MS, NCC, LPC** ("Williams") is a licensed healthcare provider serving patients in Pittsburgh, Pennsylvania.

230. Plaintiff Williams contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

231. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

232. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Williams could no longer submit claims through Therapy Notes and obtain payments for those claims. Since the shutdown, Plaintiff Heckman has had to find alternative ways to submit and resubmit claims, including submitting claims manually and collecting payments directly from her clients to continue to treat patients. Plaintiff Williams relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to herself.

233. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Williams has had to take out personal funds to meet payroll and pay other basic expenses. Plaintiff Williams has also been unable to treat patients at full capacity due to working on trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

Tennessee Plaintiff

234. Plaintiff **Heelex LLC** is a licensed healthcare provider serving patients in Knoxville, Tennessee. Heelex LLC's practice is subdivided into two medical practices, Heelex Podiatry and Heelex Medical clinics ("Heelex").

235. Plaintiff Heelex contracts with AdvancedMD, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

236. AdvancedMD, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

237. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff Heelex could no longer submit claims through AdvancedMD and obtain payments for those claims. After the shutdown and for approximately seven weeks thereafter, Plaintiff Heelex received only about one-third to one-half in payments of what it normally receives per month, despite continuing to treat patients. At one point, Plaintiff Heelex had approximately $200,000 in submitted, unpaid claims. Plaintiff Heelex relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees, and to further grow the practice, which is in jeopardy because of the Data Breach.

238. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Heelex has had to divert funds from reserves to pay operational expenses. Plaintiff Heelex's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of

Defendants' computer networks, including devoting time to submitting paper claims and tracking down Explanation of Benefits ("EOBs").

Texas Plaintiff

239. Plaintiff **Body Mind & Spine Chiropractic** ("BMSC") is a licensed healthcare provider serving patients in Temple, Texas.

240. Plaintiff BMSC contracts with ChiroTouch, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

241. ChiroTouch, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff BMSC submit their claims to ChiroTouch, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff BMSC.

242. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff BMSC could no longer submit claims through ChiroTouch and obtain payments for those claims. After the shutdown and for approximately 11 weeks thereafter, Plaintiff BMSC was not paid for any claims despite continuing to treat patients. Plaintiff BMSC has only recently started to get some payments with a majority of submitted claims remaining to be paid. Plaintiff BMSC relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

243. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff BMSC has had to take out personal funds to meet payroll and pay other basic expenses. Plaintiff BMSC's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

Washington Plaintiff

244. Plaintiff **Core Counseling and Consultation** ("CCC") is a licensed healthcare provider serving patients in Pasco, Washington.

245. Plaintiff CCC contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

246. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things.

247. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down because of the Data Breach, Plaintiff CCC could no longer submit claims through Therapy Notes and obtain payments for those claims. After the shutdown and for several weeks thereafter, Plaintiff CCC, despite continuing to treat patients, was not paid for any claims submitted. Plaintiff CCC had to switch to a different vendor to submit claims in order to receive payments for claims made. Plaintiff CCC relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to its owner and a biller.

248. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff CCC has had to take out personal funds and borrow funds to meet payroll and pay other basic expenses. Plaintiff CCC's owner has also diverted her time from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff CCC has also had to contract with another vendor to replace Therapy Notes, which has increased Plaintiff CCC's administrative costs.

Wisconsin Plaintiff

249. Plaintiff **Four Winds Counseling LLC** ("FWC") is a licensed healthcare provider serving patients in Middleton, Wisconsin.

250. Plaintiff FWC contracts with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

251. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Plaintiff FWC has been informed that Therapy Notes no longer uses Change Healthcare.

252. Beginning on or around February 21, 2024, when Defendants' computer networks were shut down, Plaintiff FWC could no longer submit claims through Therapy Notes and obtain payments for those claims. After the shutdown and for several weeks thereafter, Plaintiff FWC was not paid for any claims through a single insurer and accumulated over $100,000 in submitted, unpaid claims. Plaintiff FWC relies on the

payments it receives from submitted claims to pay basic business expenses, including salaries and wages to its owner, a biller, and contracted therapists.

253. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff FWC has had to take out a line of credit of $30,000 with an interest rate of 8.25% to meet payroll and pay other basic expenses. Plaintiff FWC's staff resources have also been diverted from treating patients at full capacity to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks. Plaintiff FWC has also had to submit claims through three separate clearinghouses to receive payments for services provided, which has increased Plaintiff FWC's administrative costs.

V. CLASS ACTION ALLEGATIONS

254. Pursuant to Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims for negligence (Count I), negligence *per se* (Count II), and unjust enrichment (Count IV), individually and on behalf of a class of all other persons similarly situated in the United States initially defined as follows:

> All healthcare providers residing in the United States whose use of Change Healthcare's services was disrupted, or whose reimbursement payments were delayed, by the Data Breach announced by UHG in February 2024 (the "Nationwide Class").

255. Pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims for negligence (Count I), negligence *per se* (Count II), negligent interference with prospective economic advantage (Count III), unjust enrichment (Count IV), and for statutory violations under various state consumer protection statutes

(Counts V-IX) as set forth below on behalf of separate states classes for Alabama, Arizona, California, Colorado, Florida, Illinois, Indiana, Iowa, Kansas, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, New Jersey, New Mexico, New York, North Carolina, Ohio, Pennsylvania, Tennessee, Texas, Washington, and Wisconsin, initially defined as follows:

> All healthcare providers residing in [name of State] whose use of Change Healthcare's services was disrupted, or whose reimbursement payments were delayed, by the Data Breach announced by UnitedHealth Group Incorporated in February 2024.

256. Additionally, pursuant to Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiffs assert a claim for breach of contract (Count IV) on behalf of a subclass defined as follows:

> All healthcare providers in the United States who contracted with Change Healthcare and utilized its services on or before February 21, 2024 ("Contract Subclass").

257. The Nationwide Class, State Classes, and the Contract Subclass are jointly referred to herein as "Class," unless otherwise stated.

258. Excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

259. Plaintiffs reserve the right to re-define the Class definitions after conducting discovery.

260. **Numerosity (Fed. R. Civ. P. 23(a)(1))**. The Class members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes over one million licensed healthcare providers. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

261. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3))**. Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to, the following:

a. Whether Defendants owed Plaintiffs and Class members a legal duty to implement and maintain reasonable security procedures and practices to protect PHI and PII;

b. Whether Defendants breached their legal duties to Plaintiffs and Class members;

c. Whether Defendants were negligent;

d. Whether Plaintiffs and Class members conferred benefits on Defendants;

e. Whether Defendants were unjustly enriched;

f. Whether Defendant Change Healthcare breached its contract;

g. Whether Defendants violated the consumer protection statutes, data breach notification statutes, state unfair insurance practice statutes, state insurance

privacy statutes, and state medical privacy statutes applicable to Plaintiffs and each of the Classes; and,

h. Whether Plaintiffs and Class members are entitled to relief, including damages and equitable relief.

262. **Typicality (Fed. R. Civ. P. 23(a)(3))**. Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the Class members. Plaintiffs, like all Class members, suffered harm because of the Data Breach and ensuing shutdown of Defendants' computer networks.

263. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4))**. Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs have retained counsel experienced in prosecuting class actions and data breach cases.

264. **Superiority (Fed. R. Civ. P. 23(b)(3))**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer

management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

265. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

a. the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Class members which would establish incompatible standards of conduct for Defendants; or

b. the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to individual Class members which would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

266. **Issue Certification (Fed. R. Civ. P. 23(c)(4))**. In the alternative, the common questions of fact and law, set forth in Paragraph 261, are appropriate for issue certification on behalf of the proposed Class members.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs, the Nationwide Class, and each of the State Classes)

267. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

268. As alleged herein, Defendants had (and continue to have) several legal duties to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their computer networks to receive and store PHI and PII provided to them by Plaintiffs and Class members, including implementing basic industry standard cybersecurity, threat detection, incident response measures, and a business continuity plan. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated. Defendants' failure to use reasonable care in securing their computer networks, including implementing basic industry standard cybersecurity, threat detection, and incident measures, was the direct and proximate cause of the shutdown that led to the interruption of Plaintiffs and Class members business operations.

269. Defendants' duty to use reasonable security measures also arose from, among other things, the special relationship that existed between Defendants and Plaintiffs and Class members, which is recognized by state and federal law, including but not limited to HIPAA. Only Defendants, however, were able to implement reasonable security measures

and to ensure that their computer networks were sufficiently secure to protect against the harm to Plaintiffs and the Class members that resulted from the Data Breach and ensuing shutdown. Yet, Defendants actively collected the PHI and PII belonging to Plaintiffs and Class members' patients, knowingly stored such data on unsecured computer networks, and once the vulnerabilities were discovered, shutdown the computer networks as a result. Plaintiffs relied on Defendants to implement reasonable security measures and to ensure that their computer networks were sufficiently secure to protect patient PHI and PII, and Defendants were aware of Plaintiffs' reliance. Defendants received an economic benefit from this special relationship.

270. A special relationship also arose because Defendants knew or should have known that PHI and PII are "highly prized" by cybercriminals, and that a large repository of PHI and PII, like Defendants' computer networks, would be a high interest target. Defendants also knew or should have known that their computer networks and cybersecurity measures were inadequate to store and safeguard PHI and PII. Therefore, the risk of a Data Breach and ransomware attack was foreseeable, and Defendants knew or should have known that their computer networks would need to be taken offline for a considerable amount of time, if vulnerabilities were discovered, causing foreseeable harm to Plaintiffs and Class Members.

271. Defendants breached their duties to Plaintiffs and Class Members, including by failing to exercise reasonable care in safeguarding their computer networks and protecting PHI and PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, audit, and test their computer networks, security processes, controls,

policies, procedures, and protocols to safeguard and protect their computer systems and PHI and PII entrusted to them, as required by applicable federal and state laws.

272. Defendants also breached their duties to Plaintiffs and Class Members by failing to implement industry standard cybersecurity, threat detection, and incident response measures, reasonably secure access controls and to implement network segmentation, by failing to restrict the amount of control a single individual could have over their computer networks, and by failing to adopt adequate incident response measures, including a business continuity plan, to ensure critical business services could be maintained after a cyberattack.

273. But for Defendants' negligent breach of the above-described duties owed to Plaintiffs and Class members, Defendants would not have experienced the data breach and would not have had to shut down their computer networks, thereby preventing Plaintiffs and Class members from (i) timely receiving payments for previously submitted claims, (ii) submitting new claims for payment, and (iii) obtaining insurance authorization for patient medical treatment, among other things. The harms to Plaintiffs and Class members were foreseeable given the types of services Defendants provide healthcare providers such as Plaintiffs and Class members and the statutory obligations shared by all to protect and maintain the security of computer networks and confidential PHI and PII.

274. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and the related shutdown, Plaintiffs and Class members have suffered (and will continue to suffer) monetary losses and economic harms and seek all available damages.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs, the Nationwide Class, and each of the State Classes)

275. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

276. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), HIPAA (42 U.S.C. §1302d *et seq*.), and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendants, had a duty to provide basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, to safeguard the PHI and PII provided to them by Plaintiffs and the Class Members.

277. Additionally, Defendants had a duty under the laws of at least fifteen states, to those respective states' Class Members, to implement and maintain basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, to safeguard the PHI and PII provided to them by Plaintiffs and the Class Members and to provide secure computer systems. The state laws include, but are not limited to, the following:

a. Alabama: Ala. Code § 8-38-1

b. California: Cal Civ. Code § 1798.81.5

c. Colorado: Col. Re. Stat. § 6-1-1301

d. Florida: Fla. Stat. § 501.171(2)

e. Illinois: 815 Ill. Comp. Stat. Ann. 530/1

f. Indiana: Ind. Code § 24-4.9-3.5 7

g. Maryland: Md. Code. Comm. Law § 14-5303

h. Massachusetts: Mass. Gen Laws Ch. 93H, § 3(a)

i. Michigan: Mich. Comp. Law 445.61

j. New Mexico: N.M. Stat. § 57-12C-1

k. New York: N.Y. Gen Bus. Law § 899-bb

l. North Carolina: N.C. Gen. Stat. § 75-60

m. Texas: Tex. Bus. & Com. Code § 521.052(a)

n. Washington: Wash. Rev. Code 19.255.020

278. Defendants breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq*.), Gramm-Leach-Bliley Act (15 U.S.C. § 6801), and the separate state reasonable data security statutes by failing to provide basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, to safeguard the PHI and PII provided to them by Plaintiffs and the Class Members.

279. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

280. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

281. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that their breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with a

breach of the Defendants' computer networks, including harms caused by shutting those systems down.

282. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
NEGLIGENT INTERFERENCE WITH PROSPECTIVE ECONOMIC ADVANTAGE
(On Behalf of Plaintiffs Riverbend Counseling Services, E5 Therapy, and the California Class)

283. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

284. Plaintiffs had an ongoing business relationship with third party businesses, including practice management companies, that would have likely resulted in future economic benefits to Plaintiffs.

285. Defendants knew or should have known about Plaintiffs' relationships with third party businesses due to the integration of Change Healthcare's services and processes with such third parties.

286. The harm to Plaintiffs resulting from the Data Breach and shutdown was foreseeable.

287. Defendants failed to act with reasonable care and engaged in wrongful conduct, including by violating like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq.),* the Gramm-Leach-Bliley Act (15 U.S.C. § 6801),

California's Confidentiality of Medical Information Act (Civil Code §56, *et seq*.), and California's Insurance Information and Privacy Protection Act (Ins. Code §791, *et seq*.).

288. The relationships between Plaintiffs and third-party businesses have been disrupted, resulting in economic harm to Plaintiffs.

289. Defendants' wrongful conduct was a substantial factor in causing the harm to Plaintiff and Class members. Plaintiffs and Class members seek all available damages.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of all Plaintiffs, the Nationwide Class, and each of the State Classes)

290. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

291. Plaintiffs and Class members conferred benefits on Defendants, both directly and indirectly, in the form of payments for claims management and processing, insurance verification, authorization and medical necessity reviews, and disbursement of payments, among other things. Defendants had knowledge of the benefits conferred by Plaintiffs and Class members and appreciated, and retained, such benefits. In accepting PHI and PII, and money from Plaintiffs and Class members, Defendants should have used, in part, the monies Plaintiffs and Class members paid to them, directly and indirectly, to pay the costs of basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan. In failing to provide such measures, the Defendants have been unjustly enriched at Plaintiffs' and Class Member's expense. Defendants had no justification for failing to provide adequate security protections.

292. Plaintiffs and Class members have suffered actual damages and harm because of Defendants' negligent, and unlawful, conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received from Plaintiffs and Class members.

COUNT V
BREACH OF CONTRACT
(On Behalf of Plaintiffs Pittsburg Internal Medicine, Ball's Rexall Drugs, Inc., and the Contract Subclass against Change under Tennessee Law)

293. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

294. Change entered contracts with Plaintiffs Pittsburg Internal Medicine, Ball's Rexall Drugs, Inc., and members of the Contract Subclass to receive and process claims for the payment of medical services and to verify insurance coverage, among other things. As part of its contractual obligations, Change was required to safeguard from unauthorized third parties and maintain confidential the PHI and PII provided to it by Plaintiff and members of the Contract Subclass in accordance with state and federal law, and to maintain its computer networks in compliance with state and federal law.

295. Change breached its contracts with Plaintiffs and members of the Contract Subclass when it failed to implement basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, which resulted in the Data Breach and related shutdown.

296. Plaintiffs and all members of the Contract Subclass members fulfilled all the terms and obligations of their contracts with Change before Change's breach.

297. As a direct and proximate result of Change's breach of the contract with Plaintiffs and members of the Contract Subclass, Plaintiffs and members of the Contract Subclass sustained damages in an amount to be determined by this Court, including interest on all liquidated sums.

COUNT VI
CALIFORNIA'S UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE § 17200*, et seq.*
(On Behalf of Plaintiffs Riverbend Counseling Services, E5 Therapy, and the California Class)

298. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

299. Defendants Change, Optum, and UHG have violated Cal. Business and Professions Code §17200 *et seq*. by engaging in unlawful or unfair business acts and practices that constitute "unfair competition" as defined in Cal. Bus. Prof. Code §17200 with respect to their failure to implement basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, thereby compromising the confidential PHI and PII provided to them by Plaintiffs and the California Class Members and the computer networks that store such confidential information.

300. Defendants' actions violating Cal. Bus. Prof. Code §17200 include, but are not limited to, engaging in unfair and unlawful acts and practices by failing to implement basic industry standard cybersecurity, threat detection, and incident response measures,

including a business continuity plan, and establishing the sub-standard security practices and procedures described herein; by soliciting and/or collecting PHI and PII from Plaintiffs and the California Class Members with knowledge that the information would not be adequately protected and that Defendants' computer networks were not secure; and, by storing PHI and PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. Defendants' practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with PHI and PII utilize appropriate security measures, as reflected by laws like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), California's Confidentiality of Medical Information Act (Civil Code § 56 *et seq*.), California's unfair insurance practices statutes (Ins. Code §790 *et seq*.), California's Insurance Information and Privacy Protection Act (Ins. Code §791 *et seq*.), and California's data breach statute, Cal. Civ. Code § 1798.81.5.

301. The above described unfair and unlawful acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

302. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, that directly and proximately caused the Data Breach and related system shutdown, Plaintiffs and California Class Members have suffered a loss of money or

property, real or personal, as described above, and will continue to suffer monetary and economic harms.

303. Defendants knew or should have known that their computer networks were unprotected and insufficient to safeguard the PHI and PII provided to them by Plaintiffs and California Class Members and that the risk of a security incident was highly likely. Defendants' actions in engaging in the above-named unlawful and unfair practices were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

304. California Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that the Defendants may have acquired by means of Defendants' unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civil Pro. §1021.5), and injunctive or other equitable relief

COUNT VII
ILLINOIS CONSUMER FRAUD AND DECEPTIVE TRADE PRACTICES ACT
815 Ill. COMP. STAT. § 505/1, *et seq.*
(On Behalf of Plaintiff Cloe Chiropractic Center and the Illinois Class)

305. Plaintiff Cloe Chiropractic Center is a person pursuant to 815 Ill. Comp. Stat. 505/1(c).

306. Defendants Change, Optum, and UHG, operate in "trade or commerce" as meant by 815 Ill. Comp. Stat. 505/1(f).

307. In the course of their businesses, Defendants Change, Optum, and UHG have violated 815 Ill. Comp. Stat. 505/2 by engaging in unfair and unlawful acts or practices with respect to their failure implement basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, to ensure that the PHI and PII entrusted to them and computer networks were not compromised by unauthorized third parties, thereby placing the confidential PHI and PII provided to them by Plaintiffs and the Illinois Class members at risk.

308. Defendants' actions violating 815 Ill. Comp. Stat. 505/2 include, but are not limited to, engaging in unfair and unlawful acts or practices by failing to implement basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, and establishing the sub-standard security practices and procedures described herein; by soliciting and/or collecting PHI and PII from Plaintiffs and the Illinois Class Members with knowledge that the information would not be adequately protected and that Defendants' computer networks were not secure; and, by storing PHI and PII in an unsecure electronic environment. Defendants' practices were contrary to duties imposed by and public policies reflected in appliable federal and state laws that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, including but not limited to laws such the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), and the Illinois Personal Information Protection Act (815 Ill. Comp. Stat. Ann. 530/1, *et seq*.) the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat 5/1014), Illinois laws

regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat 505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. 510/2(a).

309. The above unfair and unlawful acts and practices by Defendants offended public policy, were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Illinois Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

310. Defendants knew or should have known that their computer networks were unprotected and insufficient to safeguard the PHI and PII provided to them by Plaintiffs and California Class Members and that the risk of a security incident was highly likely. Defendants' actions in engaging in the above-named unlawful and unfair practices and deceptive acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and members of the Illinois Class.

311. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, that directly and proximately caused the Data Breach and related shutdown, Plaintiff and Illinois Class Members have suffered pecuniary loss, as described above, and will continue to suffer monetary and economic harms.

312. Illinois Class Members seek relief under 815 Ill. Comp. Stat. 505/10a, including, but not limited to, actual damages, punitive damages, injunctive and/or other equitable relief, restitution, and attorneys' fees and costs.

COUNT VIII
NEW MEXICO UNFAIR PRACTICES ACT
N.M. STAT. ANN. § 57-12-1, *et seq.*
(On Behalf of Plaintiff Robert Mullan, DPM, Inc. and the New Mexico Class)

313. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as is fully set forth herein.

314. Plaintiff Robert Mullan, DPM, Inc. is a person as defined by N.M. Stat. Ann. § 57-12-2.

315. Defendants Change, Optum, and UHG operate in "trade or commerce" as meant by N.M. Stat. Ann. § 57-12-2.

316. In the court of their businesses, Defendants Change, Optum, and UHG, have violated N.M. Stat. Ann. § 57-12-2 by engaging in unconscionable, unfair, and unlawful acts and practices, with respect to their failure to implement basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, to ensure that their computer networks were not compromised by unauthorized third parties, thereby compromising the confidential PHI and PII provided to them by Plaintiffs and the New Mexico Class members.

317. Defendants' actions violating N.M. Stat. Ann. § 57-12-2 include, but are not limited to, engaging in unconscionable, unfair, and unlawful acts and practices by failing to implement basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, and establishing the other sub-standard security practices and procedures described herein; by soliciting and/or collecting PHI and PII from Plaintiffs and the New Mexico Class Members with knowledge that the

information would not be adequately protected and that Defendants' computer networks were not secure; and, by storing PHI and PII in an unsecure electronic environment. Defendants' practices violated Nev. Rev. St. § 598.0923(1)(c) in that they violated duties imposed by, and public policies reflected in, appliable federal and state laws that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), the New Mexico Confidentiality of Medical Information statute (N.M. Stat. Ann. § 59A-46-27), the New Mexico Privacy of Nonpublic Personal Information regulation (N.M. Admin. Code 13.1.3); and, the New Mexico Trade Practices and Frauds in Insurance statute (N.M. Stat. Ann. §§ 59A-16-4(A), 59A-16-5)).

318. These deceptive trade practices were unconscionable pursuant to § N.M. Stat. 57-12-2(E) because they (1) took advantage of the lack of knowledge, ability, experience or capacity of the New Mexico Class Members to a grossly unfair degree; or (2) resulted in a gross disparity between the value received by a person and the price paid.

319. The above unconscionable, unfair, and unlawful acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to New Mexico Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

320. Defendants knew or should have known that their computer networks were unprotected and insufficient to safeguard the PHI and PII provided to them by Plaintiff and California Class Members and that the risk of a security incident was highly likely.

Defendants' actions in engaging in the above-named deceptive trade practices were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of the New Mexico Class.

321. As a direct and proximate result of Defendants unfair and unlawful acts and practices, that directly and proximately caused the Data Breach and related system shutdown, Plaintiff and New Mexico Class Members have suffered an ascertainable loss of money or property, real or personal, as described above, and will continue to suffer monetary and economic harms.

322. Plaintiff and the New Mexico Class Members seek relief under N.M. Stat. Ann. § 57-12-10, including, but not limited to, actual damages, injunctive and/or other equitable relief, as well as treble damages or $300, whichever is greater, and attorneys' fees and costs.

COUNT IX
WASHINGTON CONSUMER PROTECTION ACT
WASH. REV. CODE § 19.86.020, *et seq.*
(On Behalf of Plaintiff Core Counseling and Consultation and the Washington Class)

323. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as is fully set forth herein.

324. Plaintiff Core Counseling and Consultation is a person pursuant to Wash. Rev. Code § 19.86.010.

325. Defendants Change, Optum, and UHG, have violated Wash. Rev. Code § 19.86.020 by engaging in unfair and unlawful trade acts or practices in the conduct of trade or commerce, with respect to their failure to implement basic industry standard

cybersecurity, threat detection, and incident response measures, including a business continuity plan, to ensure that their data and computer networks were not compromised by unauthorized third parties, thereby compromising the confidential PHI and PII provided to them by Plaintiffs and the Washington Class Members.

326. Defendants' actions violating Wash. Rev. Code § 19.86.020 include, but are not limited to, engaging in unfair and unlawful acts or practices by failing to implement basic industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan, and establishing the sub-standard security practices and procedures described herein; by soliciting and/or collecting PHI and PII from Plaintiff and the Washington Class Members with knowledge that the information would not be adequately protected and that Defendants' computer networks were not secure; and by storing PHI and PII in an unsecure electronic environment. Defendants' practices violated duties imposed by, and public policies reflected in, applicable federal and state laws that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Washington Data Security Law (Wash. Rev. Code 19.255.020), and the Washington regulations pertaining to Privacy of Consumer Financial and Health Information (Wash. ADC 284-04-300).

327. The above unfair acts and unlawful trade practices by Defendants affect the public interest because they crippled the provision of health care services across the United States, causing substantial direct harm not only to Plaintiff Core Counseling and

Consultation but also, in the same fashion, to members of the public in Washington state and nationwide. Further, Defendants' actions were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Washington Class Members that they could not reasonably avoid and this substantial injury outweighs any benefits to consumers or to competition.

328. Defendants knew or should have known that their computer networks were unprotected and insufficient to safeguard the PHI and PII provided to them by Plaintiffs and Washington Class Members and that a cybersecurity incident, including an attack by BlackCat specifically, was highly likely. Defendants induced Plaintiff and members of the Washington Class to utilize Change Healthcare services (directly or indirectly) by failing to disclose that PHI and PII provided to Change would not be adequately protected, and that Defendants did not have a reasonable response plan in place in the event of a cyberattack. Defendants' actions in engaging in the above-named deceptive trade practices were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of the Washington Class.

329. As a direct and proximate result of Defendants' deceptive trade practices that directly and proximately caused the Data Breach and related shutdown, Plaintiffs and Washington Class Members have suffered an ascertainable loss of money or property, real or personal, as described above, and will continue to suffer monetary and economic harms.

330. Plaintiffs and Washington Class Members seek relief under Wash. Rev. Code § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive and/or other equitable relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the members of the Class defined above, respectfully request that this Court enter:

(a) An order certifying this case as a class action under Federal Rule of Civil Procedure 23, appointing Plaintiffs as the Class representatives, and appointing the undersigned as Class counsel;

(b) A judgment awarding Plaintiffs and Class members appropriate monetary relief, including damages, equitable relief, restitution, and disgorgement;

(c) An order entering injunctive and declaratory relief as appropriate under the applicable law;

(d) An order awarding Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;

(e) An order awarding reasonable attorneys' fees and costs as permitted by law; and,

(f) Any and all other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial.

Dated June 19, 2024

CIRESI CONLIN LLP

s/Jan M. Conlin

Michael V. Ciresi (#16949)
Jan M. Conlin (#192697)
Melissa A. Goodman (#330164)
Heather M McElroy (#34168X)
Barry M. Landy (#391307)
225 South Sixth Street, Suite 4600
Minneapolis, MN 55402

Phone: (612) 361-8200
Email: mvc@ciresiconlin.com
jmc@ciresiconlin.com
mag@ciresiconlin.com
hmm@ciresiconlin.com
bml@ciresiconlin.com

GIBBS LAW GROUP LLP
Eric H. Gibbs (*pro hac vice forthcoming*)
Rosemary M. Rivas (*pro hac vice forthcoming*)
David M. Berger (*pro hac vice forthcoming*)
Rosanne L. Mah (*pro hac vice forthcoming*)
Brian E. Johnson (*pro hac vice forthcoming*)
1111 Broadway, Suite 2100
Oakland, California 94607
Phone: (510) 350-9700
Email: ehg@classlawgroup.com
rmr@classlawgroup.com
dmb@classlawgroup.com
rlm@classlawgroup.com
bej@classlawgroup.com

Counsel for Plaintiffs and the Proposed Class